What is Iterated Hashing?

Pick Initial Random Value (IRV)

Hash Forward N Times

2, etc...

1.

Publish Terminal Hash Value (THV)

IRV a.k.a. H^0

H^1

H^2

H^2

$H^2 \rightarrow H^{365}$

363 Hash

THV / Terminal Hash Value

THV a.k.a. H^{365}
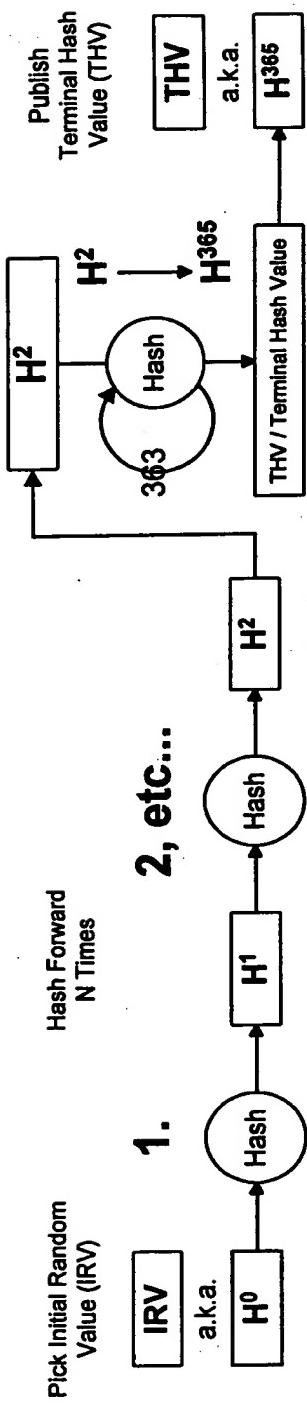
- A simple, fast, secure way to prove you know a secret.

- Hash functions are "fast" but infeasible to reverse.

- Pick a random number (IRV), hash it N times (H^0...H^N), and then publish the terminal value (THV = H^N).

- Revealing a "prior" value (H^{N-D}) proves you know IRV.

- Recipient verifies by hashing forward D times to THV.

- Effect (on a cert) is similar to issuing a fresh signature.
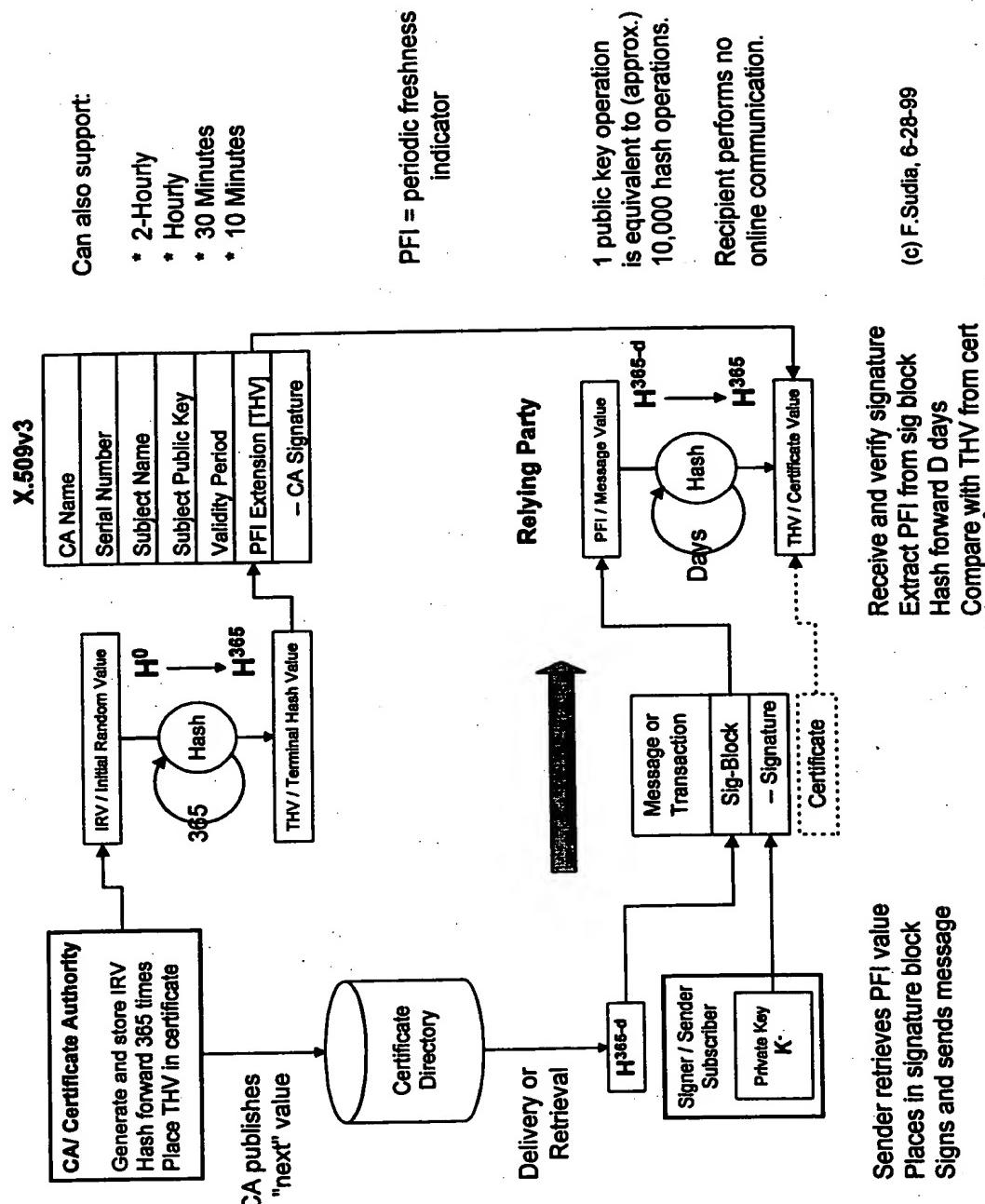
Fig. 1

Application to Secure E-Mail

X.509v3

CA Name
Serial Number
Subject Name
Subject Public Key
Validity Period
PFI Extension [THV]
— CA Signature

Can also support:

* 2-Hourly
* Hourly
* 30 Minutes
* 10 Minutes

PFI = periodic freshness indicator

1 public key operation is equivalent to (approx.) 10,000 hash operations.

Recipient performs no online communication.

(c) F.Sudia, 6-28-99

CA / Certificate Authority

Generate and store IRV
Hash forward 365 times
Place THV in certificate

IRV / Initial Random Value

$H^0 \rightarrow H^{365}$

Hash
365

THV / Terminal Hash Value

CA publishes "next" value

Certificate Directory

Delivery or Retrieval

H^{365-d}

Signer / Sender Subscriber

Private Key K

Message or Transaction
Sig-Block
— Signature
Certificate

Relying Party

PFI / Message Value

$H^{365-d} \rightarrow H^{365}$

Hash
Days

THV / Certificate Value

Sender retrieves PFI value
Places in signature block
Signs and sends message

Receive and verify signature
Extract PFI from sig block
Hash forward D days
Compare with THV from cert

Fig. 2

Application to Server Certs

(c) F.Sudia, 6-30-99

"etrade.com"

CA/ Certificate Authority
Generate and store IRV
Hash forward 365 times
Place THV in certificate

Release PFI each day

①

Web Server

Place into Unauthenticated Attribute

②

X.509v3

CA Name
Serial Number
Subject Name
Subject Public Key
Validity Period
THV Extension
-- CA Signatur
Current PFI$_x$ Value

Send server cert to Browser for SSL handshake

③

User SW Validates PFI$_x$ Against THV

④

User Browser

⑤

To make validation run even faster, user SW can cache last prior PFI$_x$

An elegant way for a bank or merchant to revoke its own server cert.

CA Name
Serial Number
Subject Name
Subject Public Key
Validity Period
THV Extension
-- CA Signature
Current PFI$_x$ Value

H^p

Fig. 3

Structure of Market

Fig. 4

Research Wkstn

Transaction Archive

Validation Processing System

Processing Phase

Online Status Responder

Business Applic.

Use Phase

Certificate Directory
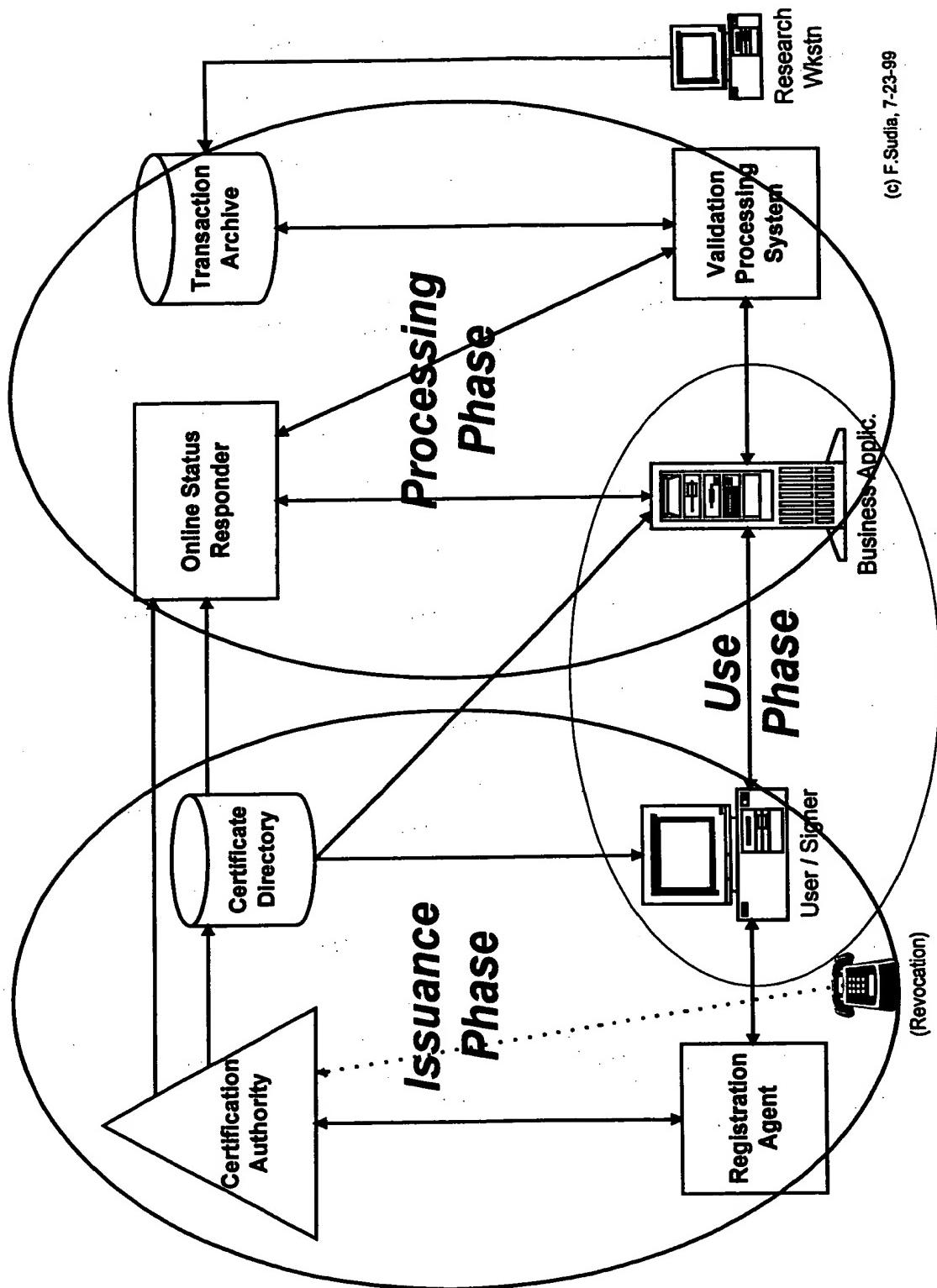
User / Signer

Issuance Phase

Certification Authority

(Revocation)

Registration Agent

(c) F.Sudia, 7-23-99